

IP VPN

Design, Concepts, Implementation

Virtual Private Networks (VPNs) make it possible to interconnect company sites via public IP networks and enable mobile users to dial in into their corporate networks. To achieve this aim, there are several VPN concepts which are discussed in this course in detail. A further focus is on making VPNs secure. The course will enable the participants to assess the pros and cons of various types of IP-based VPNs and to perform the design and implementation by themselves.

Course Contents

- Site-to-Site VPNs with IPv4 and IPv6
- GRE and Further Layer 3 Tunnel Protocols
- MPLS VPNs
- Layer 2 Tunnel Protocols for Remote Access VPNs
- Authentication and Authorization
- Voluntary Tunneling and Compulsory Tunneling
- Security in IP VPNs
- Encryption and Data Integrity
- IPsec for Site-to-Site VPNs
- Encapsulating Security Payload (ESP) and Authentication Header (AH)
- IKEv2
- IPsec for Remote Access VPNs
- SSL for Remote Access VPNs

E-Book You will receive the comprehensive documentation package of the ExperTeach Networking series – printed documentation, e-book, and personalized PDF! As online participant, you will receive the e-book and the personalized PDF.

Target Group

The course addresses network administrators and designers who are responsible for the planning and technical implementation of VPNs on the basis of different tunneling technologies in IPv4 and IPv6 networks. Attendance at this course can be credited for T.I.S.P. recertification.

Prerequisites

Profound network know-how, particularly of the TCP/IP protocol stack and the corresponding addressing and routing concepts, is required. These contents are imparted in the TCP/IP - Protocols, Addressing, Routing course.

This Course in the Web



You can find the up-to-date information and options for ordering under the following link:
www.experteach-training.com/go/IPVP

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in a non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Status 05/07/2024

Training		Prices, excl. of V.A.T.	
Classes in Germany	4 Days	€ 2,395	
Online Training	4 Days	€ 2,395	
Date/course venue	Course language	German	
23/09-26/09/24	10/03-13/03/25		
23/09-26/09/24	10/03-13/03/25		



Table of Contents

IP VPN – Design, Concepts, Implementation

1 VPN technologies - an introduction	3.4.1 Typical properties	5.1.2 The role of PPP
1.1 Why VPNs?	3.4.2 Known methods	5.1.3 VPDN - Compulsory or Voluntary Tunneling
1.1.1 Site-to-site VPNs	3.5 Authentication and authenticity	5.2 Layer 2 tunnel protocols
1.1.2 Remote access VPNs	3.5.1 Pre-shared key	5.2.1 PPTP in Microsoft networks
1.1.3 Provider solutions	3.5.2 Public key procedure	5.2.2 L2TP - The IETF Standard
1.1.4 Customer-defined VPNs	3.6 Certificates	5.3 Security in Layer 2 VPNs
1.2 VPN technologies in modern networks	3.6.1 Requesting certificates	5.3.1 Split tunneling
1.2.1 IPv4 VPNs	3.6.2 Issue certificates	5.3.2 Layer 2 IP VPNs and IPsec
1.2.2 IPv6 VPNs	3.6.3 .validity period	5.3.3 Secure Socket Tunneling Protocol (SSTP)
1.3 VPNs and security	3.6.4 Authentication	6 IPsec RAS VPNs
1.3.1 Security of provider VPNs	3.6.5 Authenticity check	6.1 Extensions for IKEv1
1.3.2 Security of customer VPNs	3.6.6 Certificate revocation list	6.1.1 The Aggressive Mode
1.4 Planning a VPN solution	3.6.7 Infrastructure	6.1.2 XAUTH - Extended Authentication
1.4.1 Separate VPN gateway	3.6.8 Public PKI	6.1.3 Hybrid Authentication
1.4.2 Firewall as VPN gateway	4 IPsec for Site-to-Site VPNs	6.1.4 IPsec and dynamic IP address assignment
2 Site-to-site VPNs	4.1 The goals of IPsec	6.2 IKEv2 in RAS VPNs
2.1 MPLS VPNs	4.2 .IPsec - The operating modes	6.2.1 Authentication with EAP
2.1.1 The customer connection	4.2.1 The Transport Mode	6.2.2 Assignment of internal addresses
2.1.2 Uniqueness of addresses	4.2.2 The Tunnel Mode	6.3 Problems with NAT or PAT
2.1.3 Directed distribution of routing information	4.3 The basic structure of IPsec	6.3.1 AH forbidden
2.1.4 LSP as a tunnel between provider edge routers	4.3.1 The Authentication Header (AH)	6.3.2 Problems with pseudoheader
2.1.5 Security against attacks	4.3.2 Encapsulating Security Payload (ESP)	6.3.3 IP address as identifier
2.1.6 IPv6 VPNs with MPLS	4.4 ISAKMP a framework	6.3.4 PAT and key renewal
2.2 VPLS - cross-site LANs and VLANs	4.5 Internet Key Exchange	6.3.5 Problems with applications
2.3 Layer 3 tunnels for networks	4.5.1 The phases of IKE	6.3.6 NAT Traversal - NAT-T
2.3.1 Tunnel interfaces	4.5.2 The Main Mode	7 SSL/TLS VPN
2.3.2 Routing in the tunnel	4.5.3 The Quick Mode	7.1 SSL/TLS - Security for TCP
2.3.3 Tunneling IPv4 over IPv4	4.6 Internet Key Exchange v2	7.1.1 The TLS protocol stack
2.3.4 Tunneling IPv6 over IPv6	4.6.1 IKEv2 - The Header	7.1.2 TLS versions and SSL
2.3.5 IPv6 in IPv4 networks	4.6.2 Tunnel structure	7.2 The TLS connection setup
2.3.6 IPv4 in IPv6 networks	4.7 Authentication options for IPsec	7.2.1 Phase 1 - Say Hello
2.3.7 Generic Routing Encapsulation (GRE)	4.7.1 Pre Shared Key	7.2.2 Phase 2 and 3 - Certificates
2.3.8 IPsec for security	4.7.2 Public key	7.2.3 Phase 4 - Completion of the handshake
3 Security for VPNs	4.8 Connection of remote stations	7.2.4 Secure data transmission
3.1 IPsec, SSL and Co. - Levels of Security	4.8.1 Problem of incompatibility	7.3 The possibilities with TLS VPNs
3.2 What does security mean?	4.8.2 Planning authentication	7.3.1 Clientless SSL VPN
3.3 Symmetric encryption	4.8.3 Use of certificates	7.3.2 Plugins as extensions
3.3.1 Lifetime of keys	5 Layer 2 VPNs	7.3.3 Tunneling applications
3.3.2 Distribution of keys	5.1 Layer 2 tunnels for dial-in clients	7.3.4 Full tunnel solution
3.4 Data integrity: hash values	5.1.1 Historically - The dial-in process	7.4 Concepts for the use of SSL VPNs

